Exercise walk-through

Data Security ▪ 6.1

eXercise

You must be able to

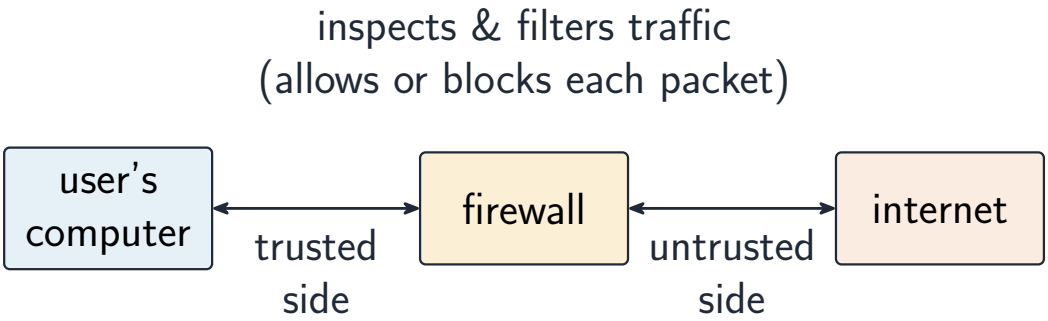
- explain the difference between **security**, **privacy** 隐私 and **integrity** 完整性
- describe the **threats** to data and systems posed by networks and the internet
- describe **security measures** for a standalone PC and for a networked system

Method — Three different ideas

Term	Means	Example failure
security	protect data from **unauthorised** access/change	a hacker reads the file
privacy	a person controls **who sees** their personal data	data shared without consent
integrity	data stays **accurate and complete**	a typo corrupts a record

All three are needed — a file can be secure but still have a typo (no integrity), or accurate but readable by anyone (no privacy).

Method — Three different ideas



A firewall is a core data-security control at the network edge

Method — Threats from the internet

Threat	What it does
virus / worm	self-copying malware (a worm spreads over the network alone)
Trojan horse	looks useful but hides malicious code
ransomware	encrypts your files and demands payment
spyware	secretly records keystrokes / passwords
phishing	fake emails/sites trick users into giving credentials
pharming 域名欺骗	redirects a user to a fake site **even when they type the correct address**
denial of service	floods a server so real users can't connect
brute-force attack	tries many passwords until one works

Method — Security measures

- **standalone PC:** strong password; up-to-date antivirus; software updates; **backup**; **encryption**; locked screen.
- **networked system:** all of the above **plus** a **firewall** 防火墙, per-user **permissions**, central account management and **audit logs**.

Practice 2.1 ▪ 2 marks

State the difference between data **security** and data **privacy**.

Solution 2.1

Method: Three different ideas

Worked steps

Security = protecting data from unauthorised access/change; privacy = the individual's right to control **who sees** their personal data B1 B1.

Practice 2.2 ▪ 1 mark

Name the type of malware that **encrypts a user's files and demands payment**.

Solution 2.2

Method: Threats from the internet

Worked steps

Ransomware B1.

Practice 2.3 ▪ 2 marks

State **two** security measures suitable for a standalone PC.

Solution 2.3

Method: Security measures

Worked steps

Any two of: strong password; up-to-date antivirus; software updates; backups; encryption; locked screen B1 B1.

Practice 2.4 ▪ 1 mark

State what a **firewall** does.

Solution 2.4

Worked steps

It monitors and controls traffic between a trusted network and an untrusted one (the internet), blocking unauthorised connections B1.

Exam-style 3.1 ▪ 3 marks

Explain the difference between **security**, **privacy** and **integrity**, giving an example of each.

Solution 3.1

Method: Three different ideas

Worked steps

Security = protection from unauthorised access (e.g. a hacker) B1; privacy = controlling who sees personal data (e.g. consent) B1; integrity = data being accurate/complete (e.g. not corrupted by a typo) B1.

Exam-style 3.2 ▪ 4 marks

Describe **two** threats posed by connecting a computer to the internet, and give a measure that reduces each.

Solution 3.2

Method: Threats from the internet

Worked steps

Any two threats, each with a measure, e.g.: malware → antivirus + updates B1 B1; phishing → user training / don't click unknown links B1 B1. *(Other valid pairs accepted.)*

Exam-style 3.3 ▪ 1 mark

(a) State what **phishing** is.
(b) State one way a user can reduce the risk of falling for a phishing attack.

Solution 3.3

Method: Threats from the internet

Worked steps

(a) Fake emails or websites that trick the user into giving away credentials/personal data B1.
(b) e.g. check the sender / don't click links in unexpected emails / type the address yourself B1.

Exam-style 3.4 ▪ 3 marks

Explain how a **firewall** and **user permissions** together help protect a networked system.

Solution 3.4

Method: Security measures

Worked steps

The firewall blocks unauthorised connections from outside B1; user permissions limit what each account can access inside B1, so even a logged-in user (or attacker) can only reach what they are allowed to B1.

Exam-style 3.5 ▪ 2 marks

State **one** difference between **phishing** and **pharming**.

Solution 3.5

Method: Threats from the internet

Worked steps

Phishing tricks the user into clicking a fake link / giving details themselves; pharming **redirects** the user to a fake site automatically even when they type the correct web address B1 B1.

Exam-style 3.6 ▪ 3 marks

A bank sends confidential statements to its customers over the internet.
(a) **Describe** how the bank uses **asymmetric encryption** so that only the intended customer can read a statement.
(b) The statement also carries a **digital signature**. **Describe** how the signature is created by the bank and checked by the customer, and **state** what it proves.
(c) A **checksum** is sent with the file as well. **Explain** what a checksum detects that a digital signature does not need to, and **state** why a checksum alone would not be enough for security.
(d) A customer's computer is infected by **malware** that records keystrokes. **Name** this type of malware and **describe** two measures that would reduce the risk.
(e) The bank also protects its own network with a **firewall**. **Describe** two things a firewall does.

Solution 3.6

Method: Threats from the internet

Worked steps

(a) The customer has a key pair and publishes the **public** key B1. The bank encrypts the statement with that public key B1. Only the customer's **private** key can decrypt it, and the customer never shares it, so nobody else can read the statement B1.
(b) The bank puts the statement through a **hashing algorithm** to produce a digest B1, then encrypts that digest with the **bank's private key** — that is the signature B1. The customer decrypts the signature with the **bank's public key** to recover the digest B1 and hashes the received statement themselves B1. If the two digests match, the statement came from the bank and has not been altered B1.

Solution 3.6

(c) A checksum detects **accidental corruption** in transmission — dropped or flipped bits B1. It is not enough for security because an attacker who alters the file can simply recompute the checksum B1; a signature cannot be forged that way, because the attacker does not have the bank's private key B1.
(d) A **keylogger**, a form of spyware B1. Any two: keep antivirus software installed and up to date; do not open attachments or install software from unknown sources; use two-factor authentication so a stolen password alone is useless; use an on-screen keyboard or a password manager for sensitive entry B1 B1.
(e) Any two: it **inspects** incoming and outgoing traffic against a set of rules and blocks whatever fails them B1; it maintains a blacklist or whitelist of addresses and ports; it can block traffic to unauthorised applications and log attempted intrusions B1.